Secrecy Throughput in Full-Duplex Multiuser MIMO Short-Packet Communications

Lai Wei, Yuli Yang, *Senior Member, IEEE*, and Bingli Jiao, *Senior Member, IEEE*

***Abstract*—In this letter, we consider the physical-layer security (PLS) in full-duplex (FD) multiuser multiple-input-multiple-output (MIMO) short-packet communications, where a base station (BS) transmits precoded signals for secure downlink multicast while receiving signals from uplink users. To quantify the PLS performance in the worst-case scenario, we consider the possible maximum wiretapping capability of a multi-antenna eavesdropper. Taking into account the self-interference (SI) in FD mode and the co-channel interference (CCI) from uplink to downlink, we analyse the secrecy throughput in finite blocklength regime and obtain its analytic expression, which perfectly matches asymptotic and simulation results in various scenarios. Moreover, the investigations on secrecy throughput substantiate that the FD multiuser MIMO systems outperform their half-duplex counterparts given the SI being sufficiently suppressed and the CCI being well managed.**

***Index Terms*—Finite blocklength, full duplex (FD), multiuser multiple-input-multiple-output (MU-MIMO), physical-layer security (PLS), short-packet communications.**

I. Introduction

In wireless communications, multiuser multiple-input-multiple-output (MU-MIMO) systems have been widely applied for simultaneous delivery of distinct signals from/to a group of peer users, for meeting the requirements on latency and capacity [1]. The design of current MU-MIMO systems mainly focuses on how to efficiently transmit long packets, based on the classical analysis framework of Shannon's convergence of optimal coding rate to channel capacity [2]. Recent information-theoretic advances in finite blocklength regime have established a basis for the design of short-packet protocols to achieve ultra-reliable low-latency communications (URLLCs) [3]. Compared with their long-packet counterparts, MU-MIMO short-packet communications bring about new communication models, and associated theoretical principles need to be addressed to assess their performance.

In addition to URLLC features, the physical-layer security (PLS) in MU-MIMO short-packet communications has attracted research interests of academics and practitioners. Specifically, half-duplex (HD) mode has been investigated in finite blocklength regime for secure MU-MIMO systems. In [4], the optimization of weighted throughput, subject to the constraints on total transmit power and bandwidth, was investigated for a secure URLLC system. In [5], a transmit power minimization problem was formulated in finite blocklength regime for a downlink MU-MIMO system. Besides, the PLS performance of a single-user downlink in mission-critical applications was studied in [6], where the optimal blocklength was derived and the impact of artificial noise was analysed.

To the best of our knowledge, the full-duplex (FD) mode has not yet been addressed in MU-MIMO short-packet communications. In finite blocklength regime, the main difference between FD and HD modes lies in the blocklength assignment. In FD mode, uplink and downlink multiplex the same blocklength. In HD mode, the accessible blocklength is divided into two orthogonal parts assigned to uplink and downlink. That is, the number of channel uses admitted in FD mode is twice that in HD mode. As is known, more available channel uses always help with the decrease in decoding error probability, which leads to a higher reliability. Motivated by this, we develop an FD transmission strategy to enhance the PLS for MU-MIMO short-packet communications.

Our main contributions in this work are three-fold. *(i)* the secrecy throughput of FD MU-MIMO systems is analysed in finite blocklength regime and obtained in an analytic form. *(ii)* Asymptotic expressions are established to obtain closed-form approximations for extreme values of blocklength, transmit power and antenna number. *(iii)* The impacts of self-interference (SI), co-channel interference (CCI) and imperfect channel state information (CSI) are taken into account.

Notations: $f_X(x)$ and $F_X(x)$ stand for the probability density function (pdf) and the cumulative distribution function (cdf) of a random variable X, respectively. Moreover, $\mathbb{E}_X(\cdot)$ denotes the expectation with respect to X. The conjugate transpose of a matrix is denoted by $(\cdot)^\dagger$. Besides, $Q(x) = (1/\sqrt{2\pi})\int_0^\infty e^{-t^2/2}\mathrm{d}t$, $\Gamma(x) = \int_0^\infty t^{x-1}e^{-t}\mathrm{d}t$ and $\Gamma(\alpha, x) = \int_x^\infty t^{\alpha-1}e^{-t}\mathrm{d}t$ are the Q-function, the gamma function and the upper incomplete gamma function, respectively.

II. System Model

Consider a secure FD MU-MIMO system shown in Fig. 1, where the FD base station (BS), having N_T transmit antennas (TAs) and N_R receive antennas (RAs), simultaneously serves K_D downlink and K_U uplink single-antenna HD legitimate users, in the presence of an N_E-antenna passive eavesdropper (Eve). Without loss of generality, we have $N_\mathrm{T} \geqslant K_\mathrm{D}$ and $N_\mathrm{R} \geqslant K_\mathrm{U}$. To maximize Eve's wiretapping capability in the interest of quantifying the maximum possible information leakage, she utilizes $N_\mathrm{E} \geqslant K_\mathrm{U}+K_\mathrm{D}$ antennas to perfectly detect the signals transmitted from uplink users and the BS.

The uplink channel matrix is denoted by $\mathbf{H}_\mathrm{U} \in \mathbb{C}^{N_\mathrm{R}\times K_\mathrm{U}}$, where the i^{th} column $\mathbf{h}_i^\mathrm{U} \in \mathbb{C}^{N_\mathrm{R}\times 1}$ contains the legitimate

L. Wei and B. Jiao are with the Department of Electronics, School of EECS, Peking University, Beijing 100871, China (e-mail: future1997@pku.edu.cn; jiaobl@pku.edu.cn).

Y. Yang (*corresponding author*) is with the School of Engineering, University of Lincoln, Lincoln LN6 7TS, U.K. (e-mail: yyang@lincoln.ac.uk).

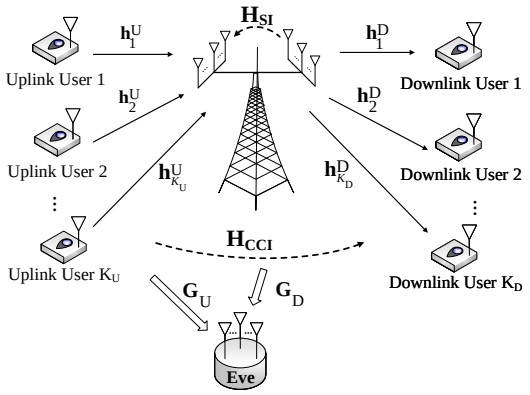

Fig. 1. Channel model of a full-duplex MU-MIMO wiretap system.

channel coefficients spanning from Uplink User i to the BS, $i \in \mathcal{K}_U = \{1, 2, \cdots, K_{\mathrm{U}}\}$. The elements in $\mathbf{h}_i^{\mathrm{U}}$ are identical and independently distributed (i.i.d.) complex Gaussian random variables with zero-mean and variance Φ_i^{U}, i.e., $\mathbf{h}_i^{\mathrm{U}} \sim \mathcal{CN}(\mathbf{0}_{N_{\mathrm{R}}\times 1}, \Phi_i^{\mathrm{U}}\mathbf{I}_{N_{\mathrm{R}}})$. The wiretapping channel in the uplink is denoted by $\mathbf{G}_{\mathrm{U}} \in \mathbb{C}^{N_{\mathrm{E}}\times K_{\mathrm{U}}}$, where the i^{th} column $\mathbf{g}_i^{\mathrm{U}} \sim \mathcal{CN}(\mathbf{0}_{N_{\mathrm{E}}\times 1}, \Psi_i^{\mathrm{U}}\mathbf{I}_{N_{\mathrm{E}}})$ is the wiretapping channel spanning from Uplink User i to Eve, $i \in \mathcal{K}_U$. In the downlink, the legitimate channel spanning from the BS to User j is denoted by an $N_{\mathrm{T}} \times 1$ vector $\mathbf{h}_j^{\mathrm{D}} \sim \mathcal{CN}(\mathbf{0}_{1\times N_{\mathrm{T}}}, \Phi_j^{\mathrm{D}}\mathbf{I}_{N_{\mathrm{T}}})$, $j \in \mathcal{K}_D = \{1, 2, \cdots, K_{\mathrm{D}}\}$. The wiretapping channel spanning from the BS to Eve is denoted by an $N_{\mathrm{E}} \times N_{\mathrm{T}}$ matrix $\mathbf{G}_{\mathrm{D}} = [g_{mn}^{\mathrm{D}}]_{N_{\mathrm{E}}\times N_{\mathrm{T}}}$, where the $(m,n)^{\mathrm{th}}$ entry $g_{mn}^{\mathrm{D}} \sim \mathcal{CN}(0, \Psi^{\mathrm{D}})$.

The residual SI at BS can be modelled as a random variable following $\mathcal{CN}(0, \varpi P_{\mathrm{B}})$ [7], where ϖ denotes the BS's capability of SI cancellation and P_{B} is the BS's total transmit power. Given the BS's SI channel $\mathbf{H}_{\mathrm{SI}} \in \mathbb{C}^{N_{\mathrm{R}}\times N_{\mathrm{T}}}$, its received signals $\mathbf{r}_{\mathrm{B}} \in \mathbb{C}^{N_{\mathrm{R}}\times 1}$ are characterised as

$$\mathbf{r}_{\mathrm{B}} = \mathbf{H}_{\mathrm{U}}\mathbf{x}_{\mathrm{U}} + \mathbf{H}_{\mathrm{SI}}\mathbf{W}\mathbf{x}_{\mathrm{D}} + \mathbf{z}_{\mathrm{B}}, \tag{1}$$

where $\mathbf{W} \in \mathbb{C}^{N_{\mathrm{T}}\times K_{\mathrm{D}}}$ is the BS's precoding matrix, and its j^{th} column $\mathbf{w}_j \in \mathbb{C}^{N_{\mathrm{T}}\times 1}$ is a linear combination of orthonormal bases in the null space of interference channels to Downlink User j. The $K_{\mathrm{U}} \times 1$ vector $\mathbf{x}_{\mathrm{U}} = [x_1^{\mathrm{U}}, x_2^{\mathrm{U}}, \cdots, x_{K_{\mathrm{U}}}^{\mathrm{U}}]^T$ contains the signals transmitted from uplink users. The $K_{\mathrm{D}} \times 1$ vector $\mathbf{x}_{\mathrm{D}} = [x_1^{\mathrm{D}}, x_2^{\mathrm{D}}, \cdots, x_{K_{\mathrm{D}}}^{\mathrm{D}}]^T$ contains the signals transmitted to downlink users. The $N_R \times 1$ vector $\mathbf{z}_{\mathrm{B}} \sim \mathcal{CN}(\mathbf{0}_{N_{\mathrm{R}}\times 1}, \sigma_{\mathrm{B}}^2\mathbf{I}_{N_R})$ contains the BS's received additive white Gaussian noise (AWGN) components.

The CCI channel matrix is denoted by $\mathbf{H}_{\mathrm{CCI}} \in \mathbb{C}^{K_{\mathrm{U}}\times K_{\mathrm{D}}}$, where the j^{th} column $\mathbf{h}_j^{\mathrm{CCI}} \sim \mathcal{CN}(\mathbf{0}_{K_{\mathrm{U}}\times 1}, \Phi_j^{\mathrm{CCI}}\mathbf{I}_{K_{\mathrm{U}}})$ contains the CCI channels from all K_{U} uplink users to Downlink User j. Thus, the signal received at Downlink User j is [8]

$$r_j^{\mathrm{D}} = (\mathbf{h}_j^{\mathrm{D}})^{\dagger}\mathbf{W}\mathbf{x}_{\mathrm{D}} + (\mathbf{h}_j^{\mathrm{CCI}})^{\dagger}\mathbf{x}_{\mathrm{U}} + z_j^{\mathrm{D}}, \tag{2}$$

where $z_j^{\mathrm{D}} \sim \mathcal{CN}(0, \sigma_j^2)$ is the AWGN at Downlink User j.

In practice, the BS utilizes zero-forcing (ZF) principles for both uplink detection and downlink transmission based on the estimated CSI $\hat{\mathbf{H}}_{\mathrm{U}} = \mathbf{H}_{\mathrm{U}} + \varepsilon\mathbf{\Delta}_{\mathrm{U}}$ and $\hat{\mathbf{h}}_j^{\mathrm{D}} = \mathbf{h}_j^{\mathrm{D}} + \varepsilon\mathbf{\Delta}_{\mathrm{D}}$, where ε is the error measure. The entries of $\mathbf{\Delta}_{\mathrm{U}} \in \mathbb{C}^{N_{\mathrm{R}}\times K_{\mathrm{U}}}$ and $\mathbf{\Delta}_{\mathrm{D}} \in \mathbb{C}^{N_{\mathrm{T}}\times 1}$ are i.i.d. and follow $\mathcal{CN}(0,1)$ [9]. As such, the BS's received signal-to-interference-plus-noise ratio (SINR) for Uplink User i, denoted by γ_i^{U}, is approximated as a Gamma-distributed random variable with shape parameter $N_{\mathrm{R}} - K_{\mathrm{U}} + 1$ and rate parameter $\rho_i^{\mathrm{U}} = P_i^{\mathrm{U}}\Phi_i^{\mathrm{U}}/(\varpi P_{\mathrm{B}} + \varepsilon^2\sum_{k\in\mathcal{K}_{\mathrm{U}}} P_k^{\mathrm{U}} + \sigma_{\mathrm{B}}^2)$ [9], where P_i^{U} is the transmit power of Uplink User i. Similarly, Downlink User j's received SINR $\gamma_j^{\mathrm{D}} \sim \mathrm{Gamma}(N_{\mathrm{T}} - K_{\mathrm{D}} + 1, \rho_j^{\mathrm{D}})$ [10] with $\rho_j^{\mathrm{D}} = P_j^{\mathrm{D}}\Phi_j^{\mathrm{D}}/(\sum_{i\in\mathcal{K}_{\mathrm{U}}} P_i^{\mathrm{U}}\Phi_j^{\mathrm{CCI}} + \varepsilon^2\sum_{k\in\mathcal{K}_{\mathrm{D}}} P_k^{\mathrm{D}} + \sigma_j^2)$, where P_j^{D} is the BS's power allocated to x_j^{D}, and $\sum_{j\in\mathcal{K}_D} P_j^{\mathrm{D}} = P_{\mathrm{B}}$.

Eve's received signals are contained by the $N_{\mathrm{E}} \times 1$ vector:

$$\mathbf{r}_{\mathrm{E}} = \mathbf{G}_{\mathrm{U}}\mathbf{x}_{\mathrm{U}} + \mathbf{G}_{\mathrm{D}}\mathbf{W}\mathbf{x}_{\mathrm{D}} + \mathbf{z}_{\mathrm{E}}, \tag{3}$$

where $\mathbf{z}_{\mathrm{E}} \sim \mathcal{CN}(\mathbf{0}_{N_{\mathrm{E}}\times 1}, \sigma_{\mathrm{E}}^2\mathbf{I}_{N_{\mathrm{E}}})$ contains Eve's AWGN components. The SINRs of x_i^{U} and x_j^{D} wiretapped by Eve are

$$\gamma_{\mathrm{E},i}^{\mathrm{U}} = \frac{P_i^{\mathrm{U}}\|(\mathbf{v}_i^{\mathrm{U}})^{\dagger}\mathbf{g}_i^{\mathrm{U}}\|^2}{\sum\limits_{\substack{k\in\mathcal{K}_{\mathrm{U}}\\ k\neq i}} P_k^{\mathrm{U}}\|\mathbf{v}_k^{\mathrm{U}}\mathbf{g}_k^{\mathrm{U}}\|^2 + \sum\limits_{l\in\mathcal{K}_D} P_l^{\mathrm{D}}\|\mathbf{v}_l^{\mathrm{D}}\mathbf{G}_{\mathrm{D}}\mathbf{w}_l\|^2 + \sigma_{\mathrm{E}}^2} \tag{4}$$

and

$$\gamma_{\mathrm{E},j}^{\mathrm{D}} = \frac{P_j^{\mathrm{D}}\|(\mathbf{v}_j^{\mathrm{D}})^{\dagger}\mathbf{G}_{\mathrm{D}}\mathbf{w}_j\|^2}{\sum\limits_{k\in\mathcal{K}_U} P_k^{\mathrm{U}}\|\mathbf{v}_k^{\mathrm{U}}\mathbf{g}_k^{\mathrm{U}}\|^2 + \sum\limits_{\substack{l\in\mathcal{K}_D\\ l\neq j}} P_l^{\mathrm{D}}\|\mathbf{v}_l^{\mathrm{D}}\mathbf{G}_{\mathrm{D}}\mathbf{w}_l\|^2 + \sigma_{\mathrm{E}}^2}, \tag{5}$$

respectively, where $\mathbf{v}_i^{\mathrm{U}}$ and $\mathbf{v}_j^{\mathrm{D}}$ denote the detection vectors for symbols x_i^{U} and x_j^{D}, respectively. If Eve obtains the BS's estimation $\hat{\mathbf{h}}_j^{\mathrm{D}}$ by wiretapping the feedback channel in downlink [11], she will be able to calculate $\mathbf{W}$. Further, to theoretically quantify the secrecy throughput in the absolute worst-case scenario where Eve has the possible maximum wiretapping capability [12], Eve's SINR is upper bounded by her signal-to-noise power ratio (SNR) in a perfect ZF detection [13]. In this case, based on the invariant law of Gaussian random vector under rotation [14], the upper bounds on Eve's wiretapping SINRs exhibit Gamma distribution, i.e., $\gamma_{\mathrm{E},i}^{\mathrm{U}} \sim \mathrm{Gamma}(N_{\mathrm{E}} - (K_{\mathrm{U}} + K_{\mathrm{D}}) + 1, \rho_{\mathrm{E},i}^{\mathrm{U}})$ and $\gamma_{\mathrm{E},j}^{\mathrm{D}} \sim \mathrm{Gamma}(N_{\mathrm{E}} - (K_{\mathrm{U}} + K_{\mathrm{D}}) + 1, \rho_{\mathrm{E},j}^{\mathrm{D}})$, where $\rho_{\mathrm{E},i}^{\mathrm{U}} = P_i^{\mathrm{U}}\Psi_{\mathrm{E},i}^{\mathrm{U}}/\sigma_{\mathrm{E}}^2$ and $\rho_{\mathrm{E},j}^{\mathrm{D}} = P_j^{\mathrm{D}}\Psi_{\mathrm{E},j}^{\mathrm{D}}/\sigma_{\mathrm{E}}^2 = P_j^{\mathrm{D}}\Psi_{\mathrm{E}}^{\mathrm{D}}/\sigma_{\mathrm{E}}^2$.

III. Multiuser MIMO Secrecy Throughput in Finite Blocklength Regime

In this section, we analyse PLS performance of FD MU-MIMO short-packet wiretap systems. Different from classical analysis of infinite blocklength framework, decoding error probability and information leakage need to be addressed concerning the finite number of channel uses. Given the blocklength N, the error probability ϵ and the information leakage δ, the maximal instantaneous secrecy rate of a wiretap system is expressed as [15]

$$R_S = \begin{cases} C_S - \sqrt{V/N}Q^{-1}(\epsilon) - \sqrt{V_{\mathrm{E}}/N}Q^{-1}(\delta), & \gamma \geqslant \gamma_{\mathrm{E}}, \\ 0, & \gamma < \gamma_{\mathrm{E}}, \end{cases} \tag{6}$$

where $C_S = \log_2(1+\gamma) - \log_2(1+\gamma_E)$ is the secrecy capacity of the wiretap system for the infinite number of channel uses, with γ and γ_{E} denoting the legitimate and wiretapping SINRs, respectively. Moreover, $V = \left(1 - 1/(1+\gamma^2)\right)(\log e)^2$ and

$V_{\mathrm{E}} = \big(1 - 1/(1+\gamma_{\mathrm{E}}^2)\big)\,(\log e)^2$ denote the channel dispersions of legitimate link and wiretapping link, respectively.

In quasi-static fading channels, for a given transmission of B information bits over the blocklength N, the error probability can be obtained by

$$\epsilon(\gamma,\gamma_{\mathrm{E}}) = Q\bigg(\sqrt{\frac{N}{V}}\big(\log_2\frac{1+\gamma}{1+\gamma_{\mathrm{E}}} - \sqrt{\frac{V_{\mathrm{E}}}{N}}Q^{-1}(\delta) - \frac{B}{N}\big)\bigg), \quad (7)$$

conditioned on $\gamma \geqslant \gamma_{\mathrm{E}}$. Note that, $\epsilon = 1$ if $\gamma < \gamma_{\mathrm{E}}$.

Leveraging the error probability, the secrecy throughput in finite blocklength regime is defined as [6]

$$T \triangleq (B/N)\big(1 - \mathbb{E}_{\gamma,\gamma_{\mathrm{E}}}(\epsilon)\big). \quad (8)$$

With this definition, the secrecy throughput of a user's information delivery in the FD MU-MIMO short-packet wiretap system under study is derived in the following theorem.

Theorem: For the delivery of B_k information bits over the blocklength N_k from/to a user k, $k \in \mathcal{K}_U \cup \mathcal{K}_D$, the secrecy throughput can be approximated as

$$T_k \approx \frac{B_k}{N_k}\bigg(\frac{\Gamma\big(M_k, \frac{\omega_k-1}{\rho_k}\big)}{\Gamma(M_k)} - \frac{(\omega_k)^{M_k}e^{-\frac{\omega_k-1}{\rho_k}}}{(\eta_k\rho_k)^{M_k}\Gamma(M_k)}\Omega_k\bigg) \quad (9)$$

where

$$\Omega_k = \sum_{m=1}^{M_k}\sum_{n=1}^{M_{\mathrm{E},k}}\tbinom{M_k-1}{m-1}\frac{(\eta_k - \eta_k/\omega_k)^{M_k-m}}{(\eta_k\rho_{E,k})^{n-1}}\frac{\Gamma(m+n-1)}{\Gamma(n)} \quad (10)$$

with $\omega_k = 2^{\frac{Q^{-1}(\delta)}{\sqrt{N_k}}+\frac{B_k}{N_k}}$ and $\eta_k = \frac{\omega_k}{\rho_k} + \frac{1}{\rho_{\mathrm{E},k}}$. For uplink users, i.e., $k \in \mathcal{K}_U$, the spatial degree of freedom (DoF) $M_k = N_{\mathrm{R}} - K_{\mathrm{U}} + 1$, and the rate parameters $\rho_k = \rho_k^{\mathrm{U}}$, $\rho_{\mathrm{E},k} = \rho_{\mathrm{E},k}^{\mathrm{U}}$. For downlink users, i.e., $k \in \mathcal{K}_D$, the spatial DoF $M_k = N_{\mathrm{T}} - K_{\mathrm{D}} + 1$ and $M_{\mathrm{E},k} = N_{\mathrm{E}} - (K_{\mathrm{U}} + K_{\mathrm{D}}) + 1$ at Eve, and the rate parameters $\rho_k = \rho_k^{\mathrm{D}}$, $\rho_{\mathrm{E},k} = \rho_{\mathrm{E},k}^{\mathrm{D}}$.

Proof: Due to the Q-function, it is hard to get a closed-form expression of the secrecy throughput. Using a linear approximation of Q-function, we approximate the error probability ϵ as [16]

$$\epsilon(\gamma,\gamma_{\mathrm{E}}) \approx \begin{cases} 0, & \gamma \geqslant \xi, \\ 1/2 - \nu\sqrt{N}\,(\gamma-\theta), & \zeta \leqslant \gamma < \xi, \\ 1, & \gamma < \zeta, \end{cases} \quad (11)$$

where $\theta = 2^{\sqrt{V_{\mathrm{E}}/N}Q^{-1}(\delta)+B/N}(1+\gamma_{\mathrm{E}}) - 1$, $\nu = 1/\sqrt{2\pi\theta(\theta+2)}$, $\zeta = \theta - 1/(2\nu\sqrt{N})$, and $\xi = \theta + 1/(2\nu\sqrt{N})$.

Subsequently, the secrecy throughput in (8) can be approximated as

$$\begin{aligned} T &= \frac{B}{N}\int_0^{+\infty}\int_{\gamma_{\mathrm{E}}}^{+\infty}\big(1-\epsilon(\gamma,\gamma_{\mathrm{E}})\big)f_{\gamma}(\gamma)f_{\gamma_E}(\gamma_{\mathrm{E}})\mathrm{d}\gamma\mathrm{d}\gamma_{\mathrm{E}} \\ &\overset{(a)}{\approx} \frac{B}{N}\int_0^{\infty}F_{\gamma_E}(\gamma_{\mathrm{E}})f_{\gamma}\big(\theta(\gamma_{\mathrm{E}})\big)\theta'(\gamma_{\mathrm{E}})\mathrm{d}\gamma_{\mathrm{E}}, \end{aligned} \quad (12)$$

where (a) is obtained by substituting (11) into (8) and leveraging the Riemann integral approximation.

Moreover, with the increase in γ_{E}, Eve's channel dispersion V_E can be approximated to 1 without losing calculation accuracy [17]. For a specific user k, we have $\theta_k(\gamma_{\mathrm{E},k}) \approx \omega_k(1+\gamma_{\mathrm{E},k}) - 1$ and $\theta_k'(\gamma_{\mathrm{E},k}) \approx \omega_k$, with $\omega_k \triangleq 2^{Q^{-1}(\delta)/\sqrt{N_k}+B_k/N_k}$.

Based on these approximations and the cdf of $\gamma_{\mathrm{E},k}$, the secrecy throughput of the information delivery pertaining to User k is approximated as

$$\begin{aligned} T_k &\approx \frac{B_k\omega_k}{N_k}\bigg(\int_0^{\infty} f_{\gamma_k}\big(\omega_k(1+\gamma_{\mathrm{E},k})-1\big)\mathrm{d}\gamma_{\mathrm{E},k} \\ &\quad - \int_0^{\infty}\sum_{n=1}^{M_{\mathrm{E},k}}\frac{(\gamma_{\mathrm{E},k})^{n-1}e^{-\frac{\gamma_{\mathrm{E},k}}{\rho_{\mathrm{E},k}}}}{\Gamma(n)(\rho_{\mathrm{E},k})^{n-1}}f_{\gamma_k}\big(\omega_k(1+\gamma_{\mathrm{E},k})-1\big)\mathrm{d}\gamma_{\mathrm{E},k}\bigg) \\ &= \frac{B_k}{N_k}\bigg(\frac{\Gamma\big(M_k,\frac{\omega_k-1}{\rho_k}\big)}{\Gamma(M_k)} - \frac{(\omega_k)^{M_k}e^{-\frac{\omega_k-1}{\rho_k}}}{(\eta_k\rho_k)^{M_k}\Gamma(M_k)}\Omega_k\bigg), \end{aligned} \quad (13)$$

where

$$\Omega_k \triangleq \int_0^{+\infty}\big(\gamma_{\mathrm{E},k} + \frac{\omega_k-1}{\omega_k}\big)^{M_k-1}\sum_{n=1}^{M_{\mathrm{E},k}}\frac{(\frac{\gamma_{\mathrm{E},k}}{\rho_{\mathrm{E},k}})^{n-1}(\eta_k)^{M_k}}{\Gamma(n)e^{\eta_k\gamma_{\mathrm{E},k}}}\mathrm{d}\gamma_{\mathrm{E},k}. \quad (14)$$

Finally, leveraging binomial expansion and the integral formula [18, (3.351-3)], the expression of Ω_k in (10) and the approximation of secrecy throughput in (9) are attained. ∎

Corollary 1: In the case of infinite blocklength, i.e., N_k goes to infinity, the secrecy throughput of User k is achieved at

$$\lim_{N_k\to\infty} T_k = \alpha_k\bigg(1-(1+\frac{\rho_k}{\rho_{\mathrm{E},k}})^{-M_k}\sum_{n=1}^{M_{\mathrm{E},k}}\frac{\Gamma(M_k+n-1)}{\Gamma(M_k)\Gamma(n)(1+\frac{\rho_{\mathrm{E},k}}{\rho_k})^{n-1}}\bigg), \quad (15)$$

where α_k denotes the coding rate of User k.

Proof: The asymptotic result in (15) is obtained by substituting $\lim_{N_k\to\infty}\omega_k = 1$ and $\lim_{N_k\to\infty}\eta_k = \frac{1}{\rho_k} + \frac{1}{\rho_{\mathrm{E},k}}$ into (9). ∎

Corollary 2: As the transmit power pertaining to the signals of User k increases, the secrecy throughput of User k, in the case of perfect CSI known by the BS, is achieved at

$$\begin{aligned} \lim_{P_k\to\infty} T_k = \frac{B_k}{N_k}\bigg(1 - \big(1+\frac{\rho_k}{\omega_k\rho_{\mathrm{E},k}}\big)^{-M_k} \\ \times\sum_{n=1}^{M_{\mathrm{E},k}}\frac{\Gamma(M_k+n-1)}{\Gamma(M_k)\Gamma(n)(1+\frac{\omega_k\rho_{\mathrm{E},k}}{\rho_k})^{n-1}}\bigg). \end{aligned} \quad (16)$$

However, if the BS's channel estimation is imperfect while Eve has a perfect detection, the secrecy throughput of User k is given by $\lim_{P_k\to\infty} T_k = 0$.

Proof: If the BS knows perfect CSI, $\lim_{P_k\to\infty}\eta_k = 0$ holds. Hence, the terms with $m < M_k$ in (10) are negligible and

$$\lim_{P_k\to\infty}\Omega_k = \sum_{n=1}^{M_{\mathrm{E},k}}\frac{\Gamma(M_k+n-1)}{\Gamma(n)(\eta_k\rho_{\mathrm{E},k})^{n-1}}. \quad (17)$$

Moreover, based on [18, (8.352-2)], we obtain

$$\lim_{P_k\to\infty}\Gamma\big(M_k,(\omega_k-1)/\rho_k\big)/\Gamma(M_k) = 1. \quad (18)$$

The limit of the secrecy throughput pertaining to User k is obtained by substituting (17) and (18) into (9).

If the BS's channel estimation is imperfect, $\lim_{P_k\to\infty}\rho_k = \Phi_k/\varepsilon^2$ and $\lim_{P_k\to\infty}\rho_{\mathrm{E},k} = +\infty$, which nullifies the terms with $n > 1$ in (10). Using [18, (8.352-2)] again, we obtain $\lim_{P_k\to\infty} T_k = 0$. ∎

Corollary 3: As the number of TAs or RAs increases, the secrecy throughput of User k is limited by

$$\lim_{M_k\to\infty} T_k = B_k/N_k. \tag{19}$$

Proof: From (10) and (14), we have

$$\begin{aligned}\Omega_k &= \sum_{m=1}^{M_k} \frac{(\eta_k-\eta_k/\omega_k)^{M_k-m}}{\Gamma(M_k-m+1)} \sum_{n=1}^{M_{\mathrm{E},k}} \frac{\Gamma(m+n-1)\Gamma(M_k)}{\Gamma(m)\Gamma(n)(\eta_k\rho_{\mathrm{E},k})^{n-1}} \\ &\le \Gamma(M_k)e^{\eta_k-\eta_k/\omega_k} M_k \sum\nolimits_{n=1}^{M_{\mathrm{E},k}} \Gamma(M_k+n-1)/\Gamma(M_k) \\ &\le \Gamma(M_k)\Gamma(M_{\mathrm{E},k})(M_k)^{M_{\mathrm{E},k}} e^{\eta_k-\eta_k/\omega_k}. \end{aligned} \tag{20}$$

Since $\Omega_k \ge 0$ and $\omega_k < \eta_k\rho_k$, we have

$$\lim_{M_k\to\infty} \frac{(\omega_k)^{M_k} e^{-\frac{\omega_k-1}{\rho_k}}}{(\eta_k\rho_k)^{M_k}\Gamma(M_k)}\Omega_k = 0. \tag{21}$$

Leveraging [18, (8.352-2)] again, we obtain

$$\lim_{M_k\to\infty} \Gamma\big(M_k, (\omega_k-1)/\rho_k\big)/\Gamma(M_k) = 1, \tag{22}$$

because $\lim_{M_k\to\infty} \sum_{i=0}^{M_k-1} [(\omega_k-1)\eta_k/\omega_k]^i/i! = e^{(\omega_k-1)\eta_k/\omega_k}$. Then, (19) is attained by substituting (21) and (22) into (9). ∎

IV. Performance Evaluation

Based on the aforementioned derivations and analysis, in this section we investigate the sum secrecy throughput defined as $\hat{T} = \sum_{k=1}^{K} T_k$, where $K \in \{K_{\mathrm{U}}, K_{\mathrm{D}}\}$, and T_k is given in (9).

In the uplink, the average received SNR of User i's signal at the BS and Eve are set to $P_i^{\mathrm{U}}\Phi_i^{\mathrm{U}}/\sigma_{\mathrm{B}}^2 = 10$dB and $P_i^{\mathrm{U}}\Psi_i^{\mathrm{U}}/\sigma_{\mathrm{E}}^2 = 0$dB, respectively, $i \in \mathcal{K}_U$. In the downlink, the BS allocates the same transmit power to all users, and the total normalized transmit power is set to $P_{\mathrm{B}}/\sigma_j^2 = 30$dB. The total normalized received power at User j and Eve are set to $P_{\mathrm{B}}\Phi_j^{\mathrm{D}}/\sigma_j^2 = 20$dB and $P_{\mathrm{B}}\Psi^{\mathrm{D}}/\sigma_{\mathrm{E}}^2 = 10$dB, respectively.

The BS's SI cancellation capability is set to $\varpi = -70$ dB [19], and the large scale fading of CCI is set to $\Phi_j^{\mathrm{CCI}} = -70$ dB, $j \in \mathcal{K}_D$ [8]. The measure of BS's channel estimation error is $\varepsilon = 5\%$ [9]. Eve has $N_E = 8$ antennas, and the information leakage is $\delta = 10^{-3}$. Monte Carlo simulation results over 10^6 channel realizations are provided to confirm the validity of our theoretical approximations and asymptotic results.

For the sake of comparison, the secrecy throughput of HD mode is investigated as well, where the information amount delivered for user k is $B_k = 1000$ bits. Given the same coding rate, both the information amount and the blocklength of a user in the FD system are twice those in the HD system.

To begin with, the impacts of the blocklength N_k, the normalized transmit power ρ^{B} and ρ^{U}, and the number of antennas, $N_{\mathrm{T}} = N_{\mathrm{R}}$, on the sum secrecy throughput $\hat{T}$ are investigated in Figs. 2, 3 and 4, where $K_{\mathrm{U}} = K_{\mathrm{D}} = 3$.

As shown in these figures, the FD MU-MIMO system achieves higher secrecy throughput than its HD counterpart as long as the SI and CCI are well managed, in both cases of perfect and imperfect CSI. The main reason behind this is that uplink and downlink in the FD system multiplex the same blocklength, whereas the HD system divides the entire

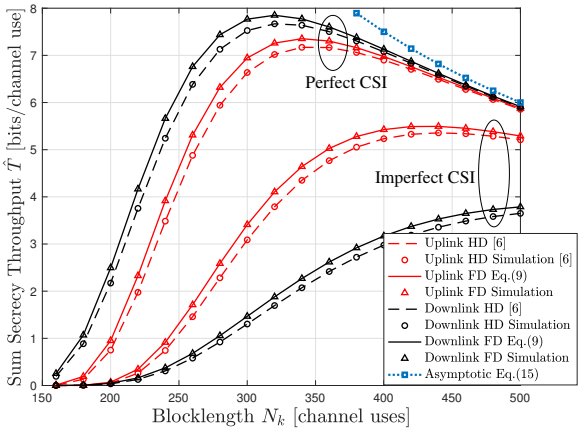

Fig. 2. Sum secrecy throughput $\hat{T}$ versus the blocklength N_k. The number of antennas at BS, $N_{\mathrm{T}} = N_{\mathrm{R}} = 8$.

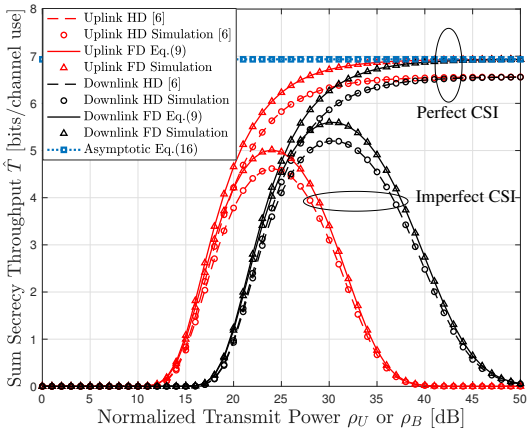

Fig. 3. Sum secrecy throughput $\hat{T}$ versus transmit power. The blocklength $N_k = 250$ channel uses in HD systems and $N_k = 500$ channel uses in FD systems. The number of antennas at BS, $N_{\mathrm{T}} = N_{\mathrm{R}} = 8$.

blocklength into two orthogonal parts to serve uplink and downlink separately. From (7), we may find that a longer blocklength leads to lower error probability, which eventually contributes to a higher secrecy throughput.

Fig. 2 reveals that the secrecy throughput is improved along with the increase of blocklength in the case of short blocklength. However, as the blocklength further increases, the secrecy throughput decreases. This phenomenon is about the tradeoff between error probability and throughput, concerning the throughput is lower if the fixed amount of information bits is delivered through longer blocklength. Moreover, since the secrecy throughput has been proved to be a quasi-concave function of blocklength in HD single-user single-antenna systems [6], an optimal blocklength can be obtained through bisection search for finding the maximum secrecy throughput, which achieves the tradeoff between latency and reliability. In MU-MIMO systems, T_k is still a quasi-concave function of N_k for each user and, therefore, the optimal blocklength can also be obtained by searching maximum $\hat{T}$. Additionally, in the case of longer blocklength, the secrecy throughput agrees

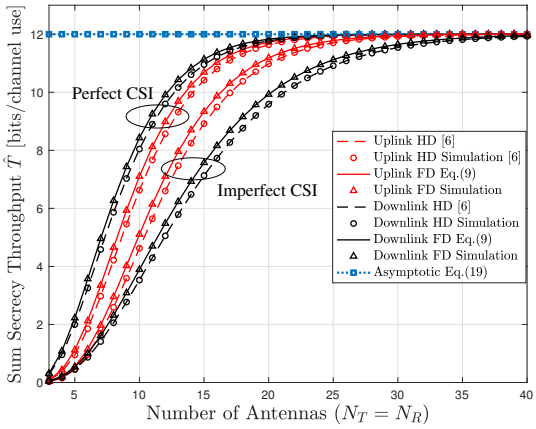

Fig. 4. Sum secrecy throughput $\hat{T}$ versus the number of TAs or RAs, $N_{\mathrm{T}} = N_{\mathrm{R}}$. The blocklength $N_k = 250$ channel uses in the HD system and $N_k = 500$ channel uses in the FD system.

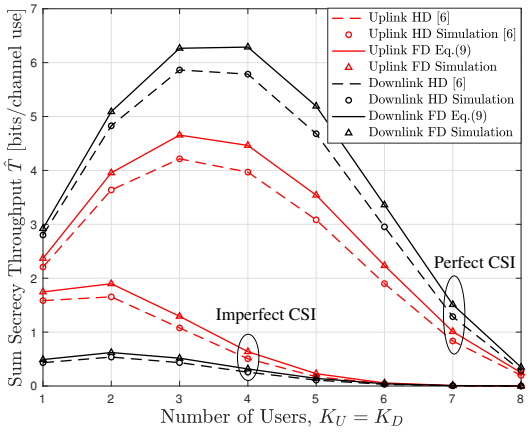

Fig. 5. Sum secrecy throughput $\hat{T}$ versus the number of users, $K_{\mathrm{U}} = K_{\mathrm{D}}$. The blocklength $N_k = 250$ channel uses in the HD system and $N_k = 500$ channel uses in the FD system. The spatial DoF of User k at Eve, $M_k = 3$.

with the asymptotic result given in *Corollary 1*.

As shown in Figs. 3 and 4, with perfect CSI, the secrecy throughput is improved as the transmit power or the number of BS's antennas increases. When the transmit power or the number of antennas goes to infinity, the secrecy throughput converges to the asymptotic results given in *Corollary 2* and *Corollary 3*, respectively. In the case of imperfect CSI, the secrecy throughput increases first and then decreases with the increase of transmit power. As the transmit power further increases, the secrecy throughput goes to zero, because legitimate SINR is limited by channel estimation error while wiretapping SINR keeps increasing. On the other hand, increasing the spatial DoF of legitimate links guarantees the convergence of secrecy throughput to asymptotic results in the case of imperfect CSI as well.

From Fig. 5, we observe that the sum secrecy throughput increases along with the number of users in the case of a few users. If the BS needs to serve many users, the sum secrecy throughput will get lower because the transmit power and spatial DoF pertaining to each user are reduced.

In addition, the comparisons in Figs. 2, 3, 4 and 5 substantiate the validity of our theoretical derivations and asymptotic results, as they match the simulation results very well.

V. Conclusion

This letter proposed a model of FD MU-MIMO short-packet wiretap systems. The PLS transmission strategy was formulated on the basis of ZF principles and the eavesdropper's wiretapping capability was maximised. To quantify the PLS performance of the FD MU-MIMO system, we derived its secrecy throughput in finite blocklength regime and obtained the analytic expression. Illustrative numerical results provided handy tools and useful references for the design of secure FD MU-MIMO short-packet systems.

References

[1] H. Zhang, M. Ma and Z. Shao, "Multi-User Linear Precoding for Downlink Generalized Spatial Modulation Systems," *IEEE Commun. Lett.*, vol. 24, no. 1, pp. 212-216, Jan. 2020.

[2] G. Durisi, T. Koch and P. Popovski, "Toward Massive, Ultrareliable, and Low-Latency Wireless Communication With Short Packets," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1711-1726, Sept. 2016.

[3] Y. Yang, "Permutation-Based Transmissions in Ultra-Reliable and Low-Latency Communications," *IEEE Commun. Lett.*, Oct. 2020.

[4] H. Ren, C. Pan, Y. Deng, M. Elkashlan and A. Nallanathan, "Resource Allocation for Secure URLLC in Mission-Critical IoT Scenarios," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5793-5807, Sept. 2020.

[5] W. R. Ghanem, V. Jamali and R. Schober, "Resource Allocation for Secure Multi-User Downlink MISO-URLLC Systems," *Proc. IEEE Int. Conf. Commun. (ICC)*, 2020, pp. 1-7.

[6] H. Wang, Q. Yang, Z. Ding and H. V. Poor, "Secure Short-Packet Communications for Mission-Critical IoT Applications," *IEEE Trans. Wireless Commun.*, vol. 18, no. 5, pp. 2565-2578, May 2019.

[7] T. M. C. Chu and H. Zepernick, "Performance of a Non-Orthogonal Multiple Access System With Full-Duplex Relaying," *IEEE Commun. Lett.*, vol. 22, no. 10, pp. 2084-2087, Oct. 2018.

[8] J. Kim, *et al.*, "Beamforming for Full-Duplex Multiuser MIMO Systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2423-2432, Mar. 2017.

[9] C. Wang, *et al.*, "On the Performance of the MIMO Zero-Forcing Receiver in the Presence of Channel Estimation Error," *IEEE Trans. Wireless Commun.*, vol. 6, no. 3, pp. 805-810, Mar. 2007.

[10] S. Akbar, *et al.*, "Massive Multiuser MIMO in Heterogeneous Cellular Networks With Full Duplex Small Cells," *IEEE Trans. Commun.*, vol. 65, no. 11, pp. 4704-4719, Nov. 2017.

[11] S. Su, *et al.*, "Data-driven mode and group selection for downlink MU-MIMO with implementation in commodity 802.11ac network," *IEEE Trans. Commun.*, Jan. 2021.

[12] Y. Liu, *et al.*, "Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access in Large-Scale Networks," *IEEE Trans. Wireless Commun*, vol. 16, no. 3, pp. 1656-1672, Mar. 2017.

[13] H. Reboredo, V. Prabhu, M. R. D. Rodrigues and J. Xavier, "Filter design with secrecy constraints: The multiple-input multiple-output Gaussian wiretap channel with zero forcing receive filters," *Proc. IEEE Int. Conf. Acoust. Speech. Signal Process. (ICASSP)*, pp. 3440-3443, May 2011.

[14] A. Shah and A. M. Haimovich, "Performance analysis of maximal ratio combining and comparison with optimum combining for mobile radio communications with cochannel interference," *IEEE Trans. Veh. Technol.*, vol. 49, no. 4, pp. 1454-1463, July 2000.

[15] W. Yang, *et al.*, "Wiretap Channels: Nonasymptotic Fundamental Limits," *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4069-4093, Jul. 2019.

[16] B. Makki, *et al.*, "Finite Block-Length Analysis of the Incremental Redundancy HARQ," *IEEE Commun. Lett.*, vol. 3, no. 5, pp. 529-532, Oct. 2014.

[17] N. Arı, *et al.*, "Average Secrecy Throughput Analysis with Multiple Eavesdroppers in the Finite Blocklength," *Proc. IEEE 31st Annu. Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, 2020, pp. 1-5.

[18] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. New York, NY, USA: Academic, 2007.

[19] S. Tian, *et al.*, "Blind Analog Interference Cancellation," *IEEE Commun. Lett.*, vol. 21, no. 8, pp. 1867-1870, Aug. 2017.